ASYMPTOTIC VALUATIONS OF SEQUENCES SATISFYING FIRST ORDER RECURRENCES

TEWODROS AMDEBERHAN, LUIS A. MEDINA, AND VICTOR H. MOLL

Abstract. Let t_n be a sequence that satisfies a first order homogeneous recurrence $t_n = Q(n)t_{n-1}$, where $Q \in \mathbb{Z}[n]$. The asymptotic behavior of the p-adic valuation of t_n is described under the assumption that all the roots of Q in $\mathbb{Z}/p\mathbb{Z}$ have nonvanishing derivative.

1. Introduction

The p-adic valuation $\nu_p(x)$, for $x \in \mathbb{Q}$, $x \neq 0$, is defined by

$$x = p^{\nu_p(x)} \frac{a}{b}, \tag{1.1}$$

where a, $b \in \mathbb{Z}$ and p divides neither a nor b. The value $\nu_p(0)$ is left undefined.

In this paper we establish the asymptotic behavior of the p-adic valuation of sequences that satisfy first order recurrences

$$t_n = Q(n)t_{n-1}, \quad n \geq 1, \tag{1.2}$$

where Q is a polynomial with integer coefficients. Among all the positive integer zeros of Q, let v be the maximum modulus. Take $n_0 > v$. Then the recurrence (1.2) is started at this index n_0. This ensures the non-vanishing of t_n. Without loss of generality, we always assume $n_0 = 0$ and $t_0 = 1$. We also adopt the notation $t_n(Q)$ while refering to the sequence defined by (1.2).

The identity

$$\nu_p(t_n(Q)) = \sum_{i=1}^{n} \nu_p(Q(i)), \tag{1.3}$$

shows that only the zeros of Q in $\mathbb{Z}/p\mathbb{Z}$ contribute to the value of $\nu_p(t_n(Q))$. The main tool of our asymptotic analysis will be Hensel's lemma. The version stated here is reproduced from [4]:

Lemma 1.1 (Hensel)**.** *Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial with coefficients in the p-adic integers $\mathbb{Z}_p$. Write $f'(x)$ for its formal derivative. If $f(x) \equiv$*

Date: February 1, 2008.
1991 *Mathematics Subject Classification.* Primary 11B37, Secondary 11B50, 11B83.
Key words and phrases. Recurrences, p-adic valuations, Hensel's lemma.

$0 \bmod p$ has a solution a_1 satisfying $f'(a_1) \not\equiv 0 \bmod p$, then there is a unique p-adic integer a such that $f(a) = 0$ and $a \equiv a_1 \bmod p$.

We now state our main theorem. This result is an asymptotic description of the valuation of the sequence t_n, defined by (1.2).

Theorem 1.2. *Let $Q \in \mathbb{Z}[n]$. Assume each of the roots of Q satisfies the hypothesis of Hensel's lemma. Let z_p denote the number of roots of Q in $\mathbb{Z}/p\mathbb{Z}$, that is,*

$$z_p := |\{b \in \{1, 2, \ldots, p\} : Q(b) \equiv 0 \bmod p\}|. \tag{1.4}$$

Then the sequence $\{t_n\}$, defined in (1.2), obeys the estimate

$$\nu_p(t_n) \sim \frac{z_p n}{p-1} \text{ as } n \to \infty. \tag{1.5}$$

Motivation. The most elementary example is $Q(x) = x$. Theorem 1.2 yields $\nu_p(n!) \sim n/(p-1)$. This follows from the classical formula of Legendre

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}, \tag{1.6}$$

where $s_p(n)$ is the sum of the digits of n in base p.

Our motivation for Theorem 1.2 comes from the study of the sequence $\{x_n\}$ defined by

$$x_n = \tan \sum_{k=1}^{n} \tan^{-1} k, \quad n \geq 1. \tag{1.7}$$

This same sequence satisfies the recursive relation

$$x_n = \frac{x_{n-1} + n}{1 - n x_{n-1}}, \tag{1.8}$$

with initial condition $x_1 = 1$. The first few values are $\{1, -3, 0, 4, -\frac{9}{19}\}$, and in [2] it was conjectured that $x_n \neq 0$ for $n \geq 4$. Later this was proved in [1] using the 2-adic valuation of x_n. The sequence $\{x_n\}$ was linked in [1] to

$$\omega_n := (1+1^2)(1+2^2)(1+3^2)\cdots(1+n^2), \tag{1.9}$$

which can be condensated as

$$\omega_n = (1+n^2)\omega_{n-1}. \tag{1.10}$$

This corresponds to $Q(x) = x^2 + 1$ and it fits into the type of recurrences considered here.

Section 2 contains the proof of Theorem 1.2 and Section 3 presentes examples illustrating the main result. In the last section we propose some future directions.

2. The proof

In the proof we assume that Q has no roots in $\mathbb{N} \cup \{0\}$. The general situation can be reduced to this one by a shift of the independent variable.

The conclusion of Theorem 1.2 is trivial if $z_p = 0$, so we assume $z_p > 0$. Denote by $b_1, b_2, \cdots, b_{z_p}$ the zeros of Q in $\mathbb{Z}/p\mathbb{Z}$. The definition of t_n yields

$$\nu_p(t_n) = \sum_{i=1}^{n} \nu_p(Q(i)). \tag{2.1}$$

All sums below are assumed to run from $i = 1$ to n.

Only the indices congruent to b_j modulo p contribute to (2.1), thus

$$\nu_p(t_n) = \sum_{i \equiv b_1 \bmod p} \nu_p(Q(i)) + \cdots + \sum_{i \equiv b_{z_p} \bmod p} \nu_p(Q(i)) \tag{2.2}$$

where $1 \leq i \leq n$. For fixed $j \in \{1,\, 2,\, \ldots,\, z_p\}$, we consider the term

$$\sum_{i \equiv b_j \bmod p} \nu_p(Q(i)). \tag{2.3}$$

Hensel's lemma produces a p-adic integer

$$\beta_j = \beta_{j,0} + \beta_{j,1}p + \cdots + \beta_{j,k}p^k + \cdots \tag{2.4}$$

such that $\beta_{j,k} \in \{0,\, 1,\, \cdots, p-1\}$, $\beta_{j,0} \equiv b_j \bmod p$ and $Q(\beta_j) = 0$. Observe that if the representation (2.4) were finite, then β_j would be a non-negative integer root of Q. This possibility has been excluded. Introduce the notation

$$\gamma_{j,s} := \beta_{j,0} + p\beta_{j,1} + p^2\beta_{j,2} + \cdots + p^s\beta_{j,s}p^s. \tag{2.5}$$

Definition 2.1. *For $n \in \mathbb{N}$, let*

$$r_n = Max\ \{j : p^j \mathit{\ divides\ some\ } Q(i) \mathit{\ for\ } 1 \leq i \leq n\}. \tag{2.6}$$

Lemma 2.2. *The sequence $r_n \to \infty$ as $n \to \infty$. Moreover, for large n, we have $p^{r_n} \leq n^{deg(Q)+1}$, hence $r_n = O(\log n)$.*

Proof. Hensel's lemma shows that $\gamma_{j,s}$ satisfies $Q(\gamma_{j,s}) \equiv 0 \bmod p^{s+1}$. For any given $M > 0$, choose an integer $s > M$. Taking $n > \gamma_{j,s-1}$ we have that $i := \gamma_{j,s-1} \in \{1,\, 2,\, \cdots, n\}$ and $p^s | Q(i)$. The definition of r_n implies that $r_n \geq s > M$. Therefore $r_n \to \infty$ as $n \to \infty$. Now observe that p^{r_n} divides $|Q(i)|$ for some $1 \leq i \leq n$. The estimate

$$p^{r_n} \leq |Q(i)| \leq \mathrm{Max}\{|Q(1)|, \cdots, |Q(n)|\} \leq Cn^{\deg(Q)} \tag{2.7}$$

gives the upper bound on r_n. The constant C depends only on the coefficients of Q. $\square$

Now

$$\sum_{i \equiv b_j \bmod p} \nu_p(Q(i)) = \sum_{i \equiv \gamma_{j,0} \bmod p} 1 + \sum_{i \equiv \gamma_{j,1} \bmod p^2} 1 + \cdots + \sum_{i \equiv \gamma_{j,r_n - 1} \bmod p^{r_n}} 1,$$

where all sums range over $1 \leq i \leq n$. The bound

$$\left\lfloor \frac{n}{p^s} \right\rfloor \leq \sum_{i \equiv \gamma_{j,s} \bmod p} 1 \leq \left\lfloor \frac{n}{p^s} \right\rfloor + 1 \tag{2.8}$$

yields

$$\begin{aligned} \sum_{i \equiv b_j \bmod p} \nu_p(Q(i)) &\geq \left(\frac{n}{p} - 1 \right) + \left(\frac{n}{p^2} - 1 \right) + \cdots + \left(\frac{n}{p^{r_n}} - 1 \right) \\ &= n \left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{n_r}} \right) - r_n \\ &= \frac{n}{p-1} \left(1 - p^{-r_n} \right) - r_n. \end{aligned}$$

Therefore

$$\frac{p-1}{n} \sum_{i \equiv b_j \bmod p} \nu_p(Q(i)) \geq 1 - p^{-r_n} - \frac{(p-1)r_n}{n}$$

and passing to the limit we conclude that

$$\liminf_{n \to \infty} \frac{p-1}{n} \sum_{i \equiv b_j \bmod p} \nu_p(Q(i)) \geq 1. \tag{2.9}$$

Similarly, using the upper bound in (2.8) we obtain

$$\sum_{i \equiv b_j \bmod p} \nu_p(Q(i)) \leq r_n + \frac{n}{p-1},$$

and it follows that

$$\limsup_{n \to \infty} \frac{p-1}{n} \sum_{i \equiv b_j \bmod p} \nu_p(Q(i)) \leq 1. \tag{2.10}$$

Therefore, Theorem 1.2 has been established.

3. Examples

In this section we present some examples illustrating Theorem 1.2.

Definition 3.1. *Given a polynomial Q and a prime p, we say that $a \in \mathbb{Z}/p\mathbb{Z}$ is a* Hensel zero *of Q if $Q(a) \equiv 0 \bmod p$ and $Q'(a) \not\equiv 0 \bmod p$. The prime p is called a* Hensel prime *for Q if all the zeros of Q in $\mathbb{Z}/p\mathbb{Z}$ are Hensel zeros. We also require that Q has at least one zero in $\mathbb{Z}/p\mathbb{Z}$. The* asymptotic zero number *is defined (provided it exists) by the limit*

$$N_p(Q) := \lim_{n \to \infty} \frac{(p-1)\nu_p(t_n)}{n}. \tag{3.1}$$

Theorem 1.2 is restated as follows:

Theorem 3.2. *Let p be a Hensel prime for Q. Then $N_p(Q) = z_p$.*

Note. The examples will show pairs (Q,p) for which $N_p(Q) \notin \mathbb{N}$. An appropriate interpretation of this number is lacking in these cases.

In the examples described below we present the *normalized error*

$$\text{err}_p(n;Q) := z_p n - (p-1)\nu_p(t_n(Q)) \tag{3.2}$$

and the *relative error*:

$$\text{relerr}_p(n;Q) := \text{err}_p(n;Q) - \text{err}_p(n-1;Q). \tag{3.3}$$

Certain regular structure of this function, as seen in Figure 3, will be analyzed in a future report.

Example 1. Let $Q(x) = x^5 + 2x^3 + 3$. Then $p = 5$ is a Hensel prime for Q. Indeed, the only zeros of Q in $\mathbb{Z}/5\mathbb{Z}$ are $a = 3$ and $a = 4$ and $Q'(a) \not\equiv 0 \bmod 5$. Theorem 1.2 gives

$$\nu_5(t_n(Q)) \sim \frac{n}{2}. \tag{3.4}$$

Figure 1 shows the valuation $\nu_p(t_n(Q))$. Figure 2 and 3 depict patterns in the normal and relative error, respectively.

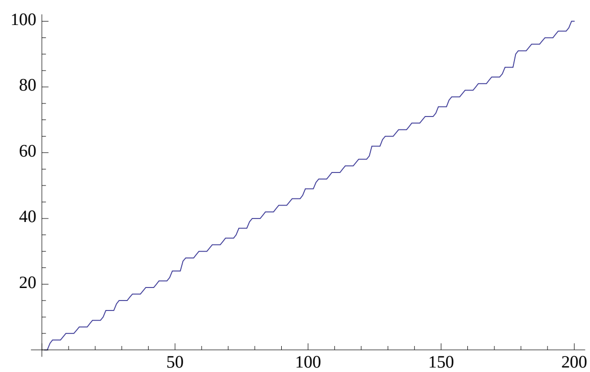

FIGURE 1. The valuation $\nu_5(t_n)$ for $Q(x) = x^5 + 2x^3 + 3$.

Example 2. A direct calculation shows that, among the first 20000 primes, $p = 3$, 11 and 29 are the only non-Hensel primes for $Q(x) = x^5 + 2x^3 + 3$. We now describe the asymptotic behavior of $\nu_p(t_n(Q))$ in each of these cases. The polynomial Q factors as

$$x^5 + 2x^3 + 3 = (x+1)H(x) \tag{3.5}$$

where

$$H(x) = x^4 - x^3 + 3x^2 - 3x + 3 \tag{3.6}$$

and the valuation splits as

$$\nu_p(t_n(Q)) = \nu_p(t_n(x+1)) + \nu_p(t_n(H(x))). \tag{3.7}$$

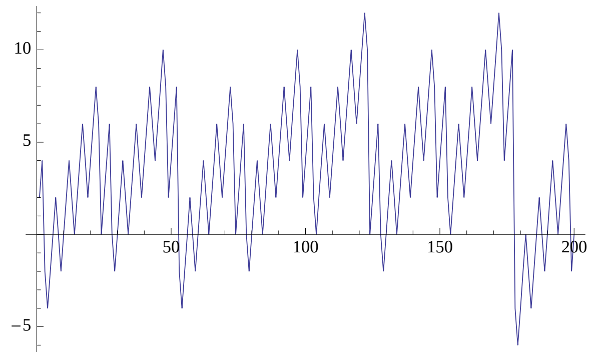

FIGURE 2. The normalized error when $p = 5$ and $Q(x) = x^5 + 2x^3 + 3$.

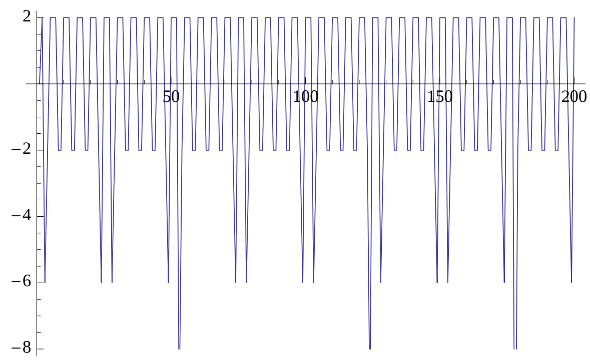

FIGURE 3. The relative error when $p = 5$ and $Q(x) = x^5 + 2x^3 + 3$.

Theorem 1.2 gives $\nu_p(t_n(x+1)) \sim n/(p-1)$, so it remains to evaluate $\nu_p(t_n(H))$.

The prime $p = 3$. In this case 0 and 1 are zeros of H in $\mathbb{Z}/3\mathbb{Z}$, and only 1 is a Hensel zero. Observe that

$$\nu_3(t_n(H)) = \sum_{j \equiv 0 \bmod 3} \nu_3(H(j)) + \sum_{j \equiv 1 \bmod 3} \nu_3(H(j)). \tag{3.8}$$

Since 1 is a Hensel zero, the argument in the proof of Theorem 1.2 implies that

$$\sum_{j \equiv 1 \bmod 3} \nu_3(H(j)) \sim \frac{n}{2}. \tag{3.9}$$

To analyze the first sum in (3.8), note that

$$H(3k) = 81k^4 - 27k^3 + 27k^2 - 9k + 3. \tag{3.10}$$

Thus, $\nu_3(H(3k)) = 1$ for $k \in \mathbb{N}$. We obtain that

$$\sum_{j \equiv 0 \bmod 3} \nu_3(H(j)) \sim \frac{n}{3}, \tag{3.11}$$

and then $\nu_3(t_n(H)) \sim \frac{5n}{6}$. Therefore $\nu_3(t_n(Q)) \sim \frac{4n}{3}$ and $N_3(Q) = \frac{8}{3}$.

The prime $p = 11$. For this prime, although Theorem 1.2 does not apply to Q itself, it is applicable to both factors $x+1$ and $H(x)$. And, we deduce

$$\nu_{11}(t_n(Q)) \sim \frac{n}{10} + \frac{2n}{10} = \frac{3n}{10}. \tag{3.12}$$

Therefore $N_{11}(Q) = 3$.

The prime $p = 29$. In order to find the asymptotic behavior of $\nu_{29}(t_n(H))$, observe that 14 is the only zero of H in $\mathbb{Z}/29\mathbb{Z}$ and

$$H(29k+14) = 36221+303601k+956217k^2+1341395k^3+707281k^4. \tag{3.13}$$

The valuations of the coefficients in $H(29k+14)$ are 1, 2, 2, 3, and 4, respectively. Therefore $\nu_{29}(H(j)) = 1$ if $j \equiv 1 \bmod 29$ and 0 otherwise. We conclude that

$$\nu_{29}(t_n(H)) \sim \frac{n}{29}. \tag{3.14}$$

Therefore $\nu_{29}(t_n(Q)) \sim \frac{57n}{812}$ and $N_{29}(Q) = \frac{57}{29}$.

Example 3. The polynomial

$$Q(x) = x^8 + x^5 + x^3 + 1 = (x^3+1)(x^5+1) \tag{3.15}$$

does not have a Hensel prime. This follows from

$$\gcd\left(Q(x), Q'(x)\right) = x+1, \tag{3.16}$$

so that, for any prime p, we have that $p-1$ is a zero of Q in $\mathbb{Z}/p\mathbb{Z}$ and $Q'(p-1) = 0$. Naturally we have

$$\nu_p(t_n(Q)) = \nu_p(t_n(x^3+1)) + \nu_p(t_n(x^5+1)). \tag{3.17}$$

The asymptotic behavior of $\nu_p(t_n(Q))$ is discussed next.

Lemma 3.3. *Let p be an odd prime and $x \neq 1$. Then*

$$\nu_p(x^p - 1) = \begin{cases} 0 & \text{if } x \not\equiv 1 \bmod p \\ 1 + \nu_p(x-1) & \text{if } x \equiv 1 \bmod p. \end{cases} \tag{3.18}$$

Proof. The first part is clear from the congruence $x^p \equiv x \bmod p$. To verify the second assertion, write $x = kp+1$ and observe that

$$\nu_p(x^p - 1) = \nu_p\left(\sum_{r=1}^{p} \binom{p}{r} k^r p^r \right). \tag{3.19}$$

For $r > 1$, the p-adic valuation of each term in the sum is greater than $2 + \nu_p(k)$. When $r = 1$, it is exactly $2 + \nu_p(k)$. Then, putting $k = \frac{x-1}{p}$ verifies the assertion. $\square$

Corollary 3.4. *Let p be an odd prime and $x \in \mathbb{Z}$, $x \neq 1$. Define*

$$T_p(x) = x^{p-1} + x^{p-2} + \cdots + 1. \tag{3.20}$$

Then

$$\nu_p(T_p(x)) = \begin{cases} 0 & \text{if } x \not\equiv 1 \bmod p \\ 1 & \text{if } x \equiv 1 \bmod p. \end{cases} \tag{3.21}$$

Corollary 3.5. *Let p be a prime and $x \in \mathbb{Z}$, $x \neq -1$. Then*

$$\nu_p(x^p + 1) = \begin{cases} 0 & \text{if } x \not\equiv -1 \bmod p \\ 1 + \nu_p(x+1) & \text{if } x \equiv -1 \bmod p. \end{cases} \tag{3.22}$$

Proof. Replace x by $-x$ in Lemma 3.3. □

Corollary 3.6. *Let p be a prime and $x \in \mathbb{Z}$, $x \neq -1$. Define*

$$S_p(x) = x^{p-1} - x^{p-2} + \cdots - x + 1. \tag{3.23}$$

Then

$$\nu_p(S_p(x)) = \begin{cases} 0 & \text{if } x \not\equiv -1 \bmod p \\ 1 & \text{if } x \equiv -1 \bmod p. \end{cases} \tag{3.24}$$

The number of roots of $x^q + 1 \equiv 0 \bmod p$, that is, $z_p(x^q+1)$ stated in the Lemma below appears at the end of Section 8.1 of [3].

Lemma 3.7. *Let p and q be primes. The number of solutions of the congruence $x^p + 1 \equiv 0 \bmod q$ is $gcd(p, q-1)$.*

Corollary 3.8. *Let p be an odd prime. Then*

$$\nu_p(t_n(x^p \pm 1)) \sim \frac{(2p-1)n}{p(p-1)}. \tag{3.25}$$

If q is a prime, $q \neq p$, then

$$\nu_q(t_n(x^p \pm 1)) \sim \frac{gcd(p, q-1)\, n}{q-1}. \tag{3.26}$$

Proof. Theorem 1.2 gives $\nu_p(t_n(x+1)) \sim \frac{n}{p-1}$. The expression for $\nu_p(S_p(x))$ yields $\nu_p(S_p(x)) \sim n/p$. The asymptotic behavior of $\nu_q(t_n(x^p \pm 1))$ follow directly from Theorem 1.2. □

We now complete the analysis of

$$\nu_p(t_n(Q)) = \nu_p(t_n(x^3+1)) + \nu_p(t_n(x^5+1)). \tag{3.27}$$

If $p \neq 3$ is a prime, then

$$\nu_p\left(t_n(x^3+1)\right) \sim \frac{z_p(x^3+1)\, n}{p-1}. \tag{3.28}$$

Similarly, for $p \neq 5$ prime, we have

$$\nu_p\left(t_n(x^5+1)\right) \sim \frac{z_p(x^5+1)\,n}{p-1}. \tag{3.29}$$

Thus, (3.25) and (3.29) yield

$$\nu_3(t_n(Q)) \sim \nu_3(t_n(x^3+1)) + \nu_3(t_n(x^5+1)) = \frac{5n}{6} + \frac{n}{2} = \frac{4n}{3}.$$

Similarly, $\nu_5(t_n(Q)) \sim 7n/10$.

Now let $p \neq 3,\, 5$ be a prime. Theorem 1.2 now applies directly to give

$$\nu_p(t_n(Q)) \sim \frac{\left[z_p(x^3+1) + z_p(x^5+1)\right]\, n}{p-1}. \tag{3.30}$$

Lemma 3.7 yields

$$\nu_p(t_n(Q)) \sim \frac{[\gcd(3,p-1) + \gcd(5,p-1)]\; n}{p-1}. \tag{3.31}$$

The asymptotic zero number is given by

$$N_p((x^3+1)(x^5+1)) = \begin{cases} \frac{8}{3} & \text{if } p = 3 \\ \frac{14}{5} & \text{if } p = 5 \\ \gcd(3,p-1)+\gcd(5,p-1) & \text{if } p \neq 3,\, 5. \end{cases} \tag{3.32}$$

Example 4. Let p be an arbitrary prime and define

$$A_p(x) = (px+1)^2\left((p+1)x+1\right). \tag{3.33}$$

A direct calculation shows that p is the only Hensel prime for A_p. Therefore

$$\nu_p(t_n(A_p)) \sim \frac{n}{p-1}. \tag{3.34}$$

To compute the asymptotics for a prime $q \neq p$, let $Q_1(x) = px+1$ and $Q_2(x) = (p+1)x+1$, and observe that

$$\nu_q(t_n(A_p)) = 2\nu_q(t_n(Q_1)) + \nu_q(t_n(Q_2)). \tag{3.35}$$

Theorem 1.2 applies to both Q_1 and Q_2. The case for Q_1 is immediate since $px+1 \equiv 0 \bmod q$ has a unique solution. To evaluate $\nu_q(t_n(Q_2))$ observe that the number of solutions of $(p+1)x+1 \equiv 0 \bmod q$ is 0 or 1, according to whether q divides $p+1$ or not. Thus

$$\nu_q(t_n(A_p)) \sim \frac{(2+\omega_{p,q})n}{q-1} \tag{3.36}$$

where

$$\omega_{p,q} = \begin{cases} 1 & \text{if } q \text{ divides } p+1, \\ 0 & \text{otherwise.} \end{cases}$$

We conclude that

$$N_q(A_p) = \begin{cases} 1 & \text{if } p = q, \\ 2 + \omega_{p,q} & \text{if } p \neq q. \end{cases} \tag{3.37}$$

4. Future directions

In this section we outline certain generalizations of the main result of the paper.

A natural extension of Theorem 1.2 deals with the situation in which there is an element $b \in \mathbb{Z}/p\mathbb{Z}$ such that

$$Q(b) \equiv Q'(b) \equiv \cdots \equiv Q^{(k-1)}(b) \equiv 0 \bmod p. \tag{4.1}$$

The question of how the multiplicities of the roots enter in the asymptotic behavior of $\nu_p(t_n(Q))$ appears to be a salient quest, and this will be addressed elsewhere.

Another interesting continuation of the ideas presented in this paper would be the study of p-adic valuation of sequences satisfying second order recurrences

$$t_n = Q_1(n)t_{n-1} + Q_2(n)t_{n-2}, \tag{4.2}$$

with polynomials Q_1 and Q_2. This problem includes, classically, the case of Fibonacci and Stirling numbers.

Acknowledgments. The work of the third author was partially funded by NSF-DMS 0409968. The second author was partially supported as a graduate student by the same grant.

References

[1] T. Amdeberhan, L. Medina, and V. Moll. Arithmetical properties of a sequence arising from an arctangent sum. To appear in *Journal of Number Theory*, 2007.
[2] G. Boros and V. Moll. Sums of arctangents and some formulas of Ramanujan. *Scientia*, 11:13–24, 2005.
[3] K. Ireland and M. Rosen. *A classical introduction to Number Theory*. Springer Verlag, 2nd edition, 1990.
[4] M. Ram Murty. *Introduction to p-adic Analytic Number Theory*, volume 27 of *Studies in Advanced Mathematics*. American Mathematical Society, 1st edition, 2002.

Department of Mathematics, Tulane University, New Orleans, LA 70118
E-mail address: tamdeber@tulane.edu

Department of Mathematics, Tulane University, New Orleans, LA 70118
E-mail address: lmedina@math.tulane.edu

Department of Mathematics, Tulane University, New Orleans, LA 70118
E-mail address: vhm@math.tulane.edu